KPMG

The Next Transformation

Zero Trust

18 November 2021

Contents

1

Zero Trust – The case for change

What is driving Zero Trust adoption...

Innovation, digital transformation, supply chain and **remote productivity** require employees, contractors, suppliers and ecosystem of partners to **access enterprise applications securely** from **anywhere, any device and at anytime**.

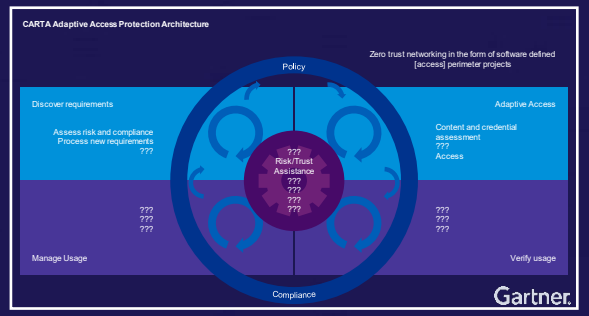
The different Zero Trust models

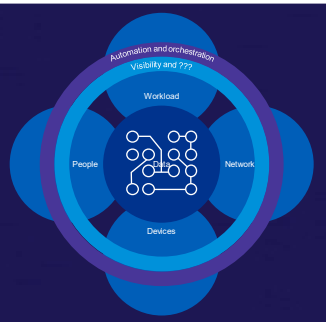
US Government Executive Order, May, 2021 - 60 days for agencies to plan Zero Trust architecture

NCSC (UK) launch Zero Trust 1.0 July, 2021

Zero Trust Historical Timeline

- **2004** The Jericho Forum De-Perimeterization
- **2009** Forrester Coins "Zero Trust"
- **2014** Google Publishes "BeyondCorp"
- **2015** Technology Vendors begin to multiply
- **2017** Forrester Releases ZTX Gartner Releases CARTA
- **2020** NIST Publishes Zero Trust 800-207
- **Today's Zero Trust**





The concept od Zero Trust can be seen in **Gartner's CARTA** model – continuous adaptive risk and trust assessment. This calls for a shift away from one-time, binary access decisions and toward contextual, risk and trust-based decision. This model is about giving just enough trust to users, even after authentication, to complete the action requested.

Forrester's Zero Trust eXtended (ZTX) refers to breaking down "monolithic perimeters" into a series of micro-perimeters or network segments to apply granular security controls around them. But they also acknowledge that it's mush more than just network segmentation – it's a holistic approach to securing data, network, device, workloads and workforces.

Google's BeyondCorp is their implementation of zero-trust architecture that requires securely identifying the user and device, removing trust from the network, externalizing apps and workflow, and implementing inventory-based access control

The above models provide a good reference starting point, however a enterprise's own ZT definition and model needs to be customized. Also, ZT across different ecosystems can be different level of maturity i.e., your cloud vs on-prem vs. hybrid environments will enables different feature of a ZT architecture.

KPMG

The level set

THE NEW PARADIGM: NEVER TRUST. ALWAYS VERIFY. LEAST PRIVILEGE

DEFINITION

- "Zero Trust," a security model that constitutes a more data-centric and identity aware approach that is designed to handle the new challenges of our "perimeter-everywhere" world
- Zero Trust is driven by the precepts of never trusting anything inside nor outside the organization's security perimeters
- Before access is granted, anything and everything that is attempting to connect to an organization's systems must always be verified

APPROACH

- Implementing a ZT strategy is not something you do once and cookie-cutter copy from network to network because each environment and protect surface is different
- Leverage existing efforts around IAM, endpoint strategy and network segmentation work to build the business case for ZT transformation
- Tackle cloud environments and applications first for easy enablement followed by modern app stack on prem

OUTCOMES

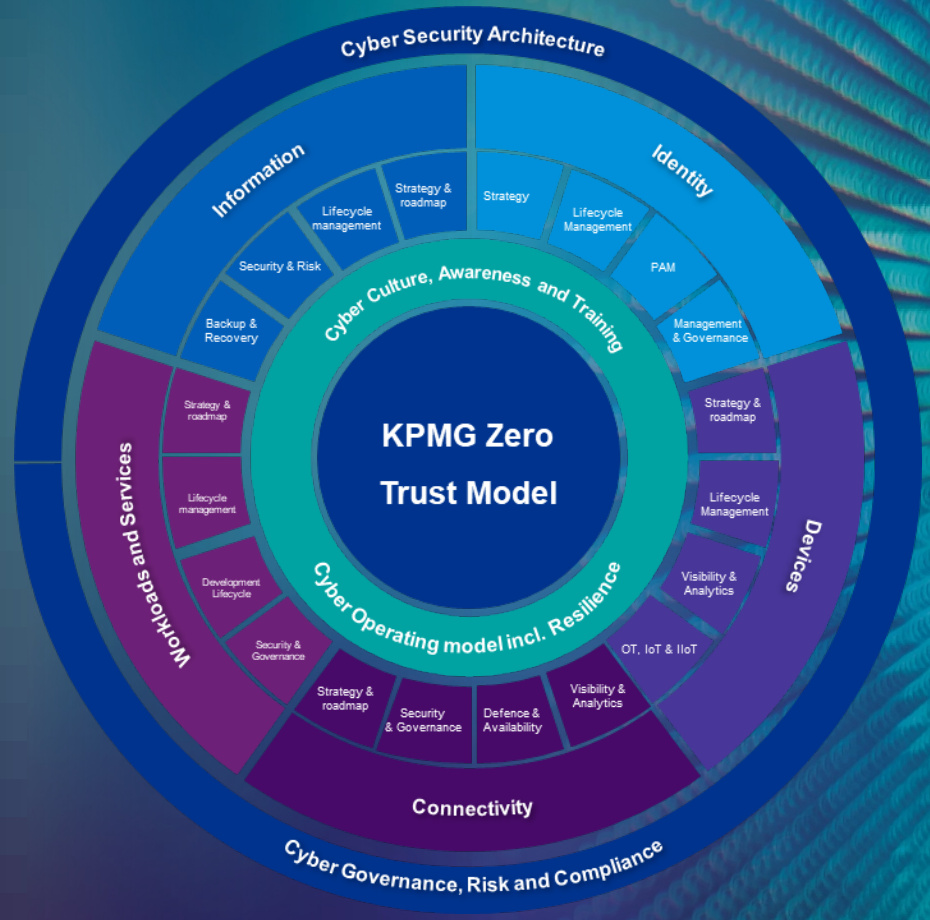
- Overall simplification of security architecture tightly coupled with your application and infrastructure roadmaps
- Improved and more trusted User experience
- Simplifies operations through automation and a reduced rule base, and simplifies regulatory compliance and audits

2

Principles and framework

Principles

Principles are lynchpin to Zero Trust. All solutions should embrace multiple of them to align with the overall enterprise vision of Zero Trust.



Note: Dynamic context, Automation and Orchestration are assumed capabilities within most technologies that have embraced a Zero Trust approach.

From Project to Zero Trust Transformation

Cyber outcomes

IAM

Identity issues:

We help clients carry out identity transformation and Privilege access management solutions

Network

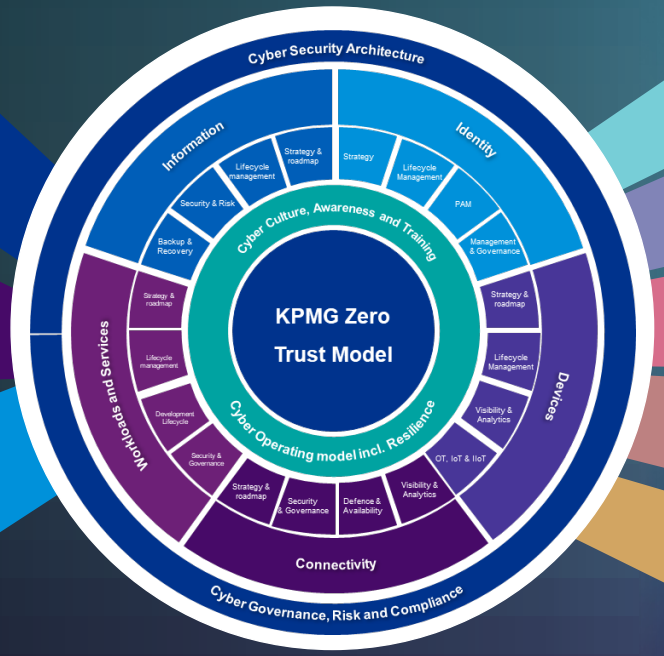
Lateral Movement: We help our clients carry out network transformations e.g. VPN to Private access, MPLS replacements, etc.

Data

Regs & Data Security:

We help our clients address data security & privacy issues to comply with regulatory requirements

Zero Trust approach



Business outcomes

01 **Easier M&A**
Identity, Connectivity, Cloud and Information transformation…

02 **Business collaboration**
Identity, Devices, Connectivity, Workloads & Services and Information

03 **Digital Transformation**
Identity, Connectivity, Workloads & Services and Information

04 **Remote working**
Identity, Devices, Connectivity, Workloads & Services and Information

05 **Reduce business risk**
Identity, Devices, Connectivity, Workloads & Services and Information

3

Key risks and opportunities for Risk and Audit

The future of security will be...Zero Trust

Enabling **secure**, **fast and easy** experiences from anywhere

Able to predict and plan **defenses in real time**

Innovative and agile

Strategic enabler of the business

Proactive risk management

Digitized and **automated**

Fast and fluid deployment of resources

Insight-driven/ data, analytics, etc.

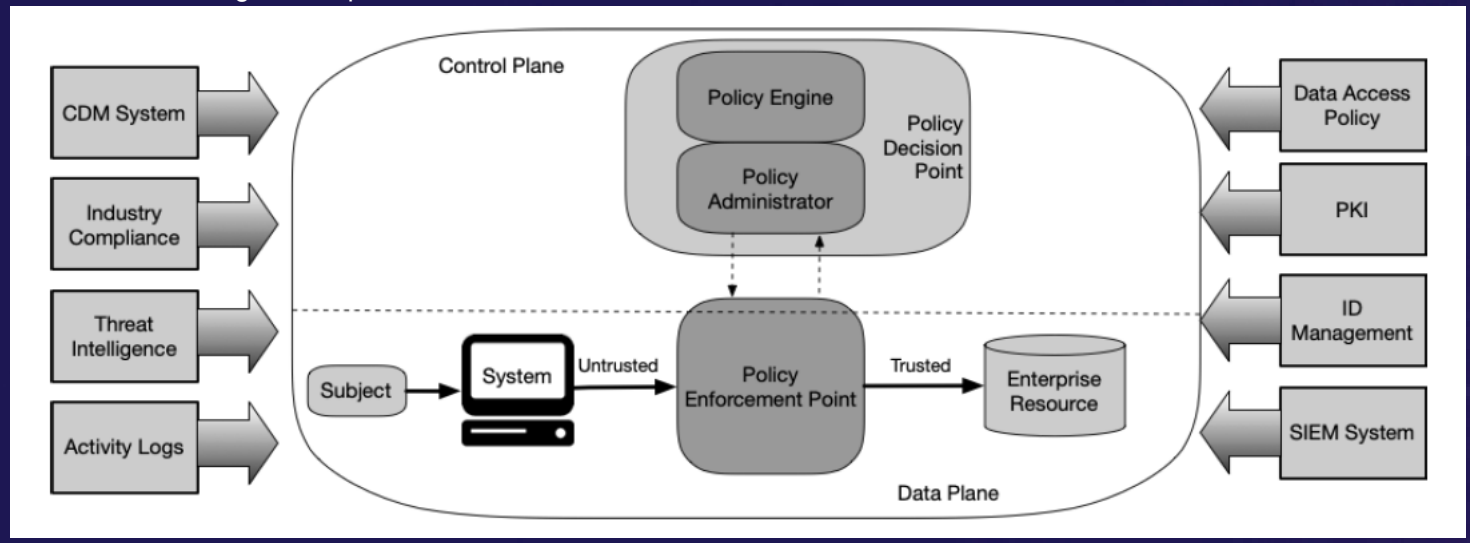
Strong **mobility enabled**

Centralization of policy enforcement

Zero Trust relies heavily on the **Policy engine.** This is a key point for attention, as many decisions will be **automated.** This is both a blessing and a curse. As auditors and risk professionals, this should be a key asset of interest for **assessments.**

Secondary to this **enforcement** will be mainly automated, and potentially using **AI** and **algorithms** to cross reference many sources. This might proof a **challenge** for assessment. Its paramount to identify the "**golden source**" of data used.

Core zero Trust logical components



Source: NIST SP 800-207 (figure 2)

Zero Trust and DevOps

DevOps' code persistence, resilience and security is a direct reflection of how well integrated Zero Trust security design principles are in every phase of the System Development Lifecycle (SDLC). But when development and operations become "one", segregation of duties becomes a challenge…

- **RBAC and Least privileged** using service mesh technologies (an overlay network that sits between services)
- **Reporting:** Design in a series of automated audit reporting points across the combined DevOps and Zero Trust framework to automate compliance reporting and ensure sensitive data is secure
- **API discovery and management:** discover app APIs and create authorization policies to simplify access
- **Certificate management:** Strive towards standing up a service for certificates so that this infrastructure can be leveraged across many teams. This gives security teams a central point of control to set guardrails and monitor issuance while making things a lot easier for developers.
- **Source Code Management or SCM:** maintain a track of versions (revisions) made to the program. Each version has a timestamp and the person who made the changes. These versions can be compared and merged. SCM is also known as Version Control.
- **Continuous code inspection:** Tools that will continuously scan through source code, allowing development teams to spot bugs and fix vulnerabilities that compromise their apps, to keep undefined behavior from impacting end-users.

4

Transforming Risk and Audit

Internal audit trusted, and disrupted

All these forces are driving extensive organizational transformation and, in turn, disrupting internal audit.

Shifting regulations, social expectations and cultural understanding

Rapidly changing technology and digital acceleration

Talent shortages and team expectations

Budgetary pressures

Emerging risks

Unprecedented changes in business and operating models

The future Chief Audit Executive (CAE) Agenda

Leading organizations have developed an agenda to help deal with disruption across their internal audit functions.

The highlighted areas are of particular importance with respect to building readiness for a Zero Trust environment.

Stakeholder engagement and trust

Internal audit knows its top stakeholders and takes the time to foster a relationship of trust attuned to their needs

Digital acceleration

Leverage technology with organizational goals in mind, and use it to enable program and project level work

Data, analytics and insights

Enterprise data is available and used, and new data is curated by internal audit. This data is used to provide risk insights and enhanced assurance through broader audit coverage

Strategy and value management

Internal audit strategy considers a mix of enhanced assurance, risk insights and business improvements attuned to stakeholder needs. Strategically important and future-focused emerging risks are prioritized

New ways of working

Where services are delivered, the competencies that enable that delivery, and the way audit teams want to work has to be revisited to help retain the right talent

Operating model agility

Audit activities are responsive to disruption, flex with the business strategy throughout the year, and consider coordination with other lines of defense

Data, analytics, and insights

Use of data analytics continues to be a powerful tool for the internal audit function to help assess risk and provide insights to assist management decision-making on process improvements and control effectiveness.

The opportunity becomes even greater with the adoption of Zero Trust.

Enterprise data is leveraged for risk insights and action

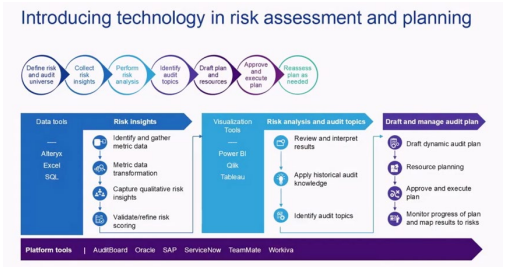
- Data analytics and technology can enable internal audit risk assessment, planning and monitoring **by**:
- Aggregating relevant enterprise information
- Automating the flow of information into insights

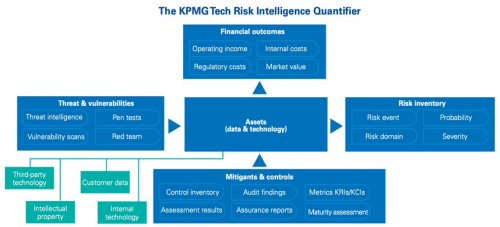
Audit coverage is broader than ever before, with risk appetite in mind

- Data analytics and technology can support broader audit coverage and continuous auditing **by**:
- Offering visibility to trends across an entire population
- Allowing internal audit to target its approach more meaningfully

Data driven risk assessment enables smarter decision making

- Leverage risk to help make smarter business decisions with data-driven risk assessment, specific to technology risk domains
- Utilizing data science to better understand and make decisions about risk





Digital acceleration

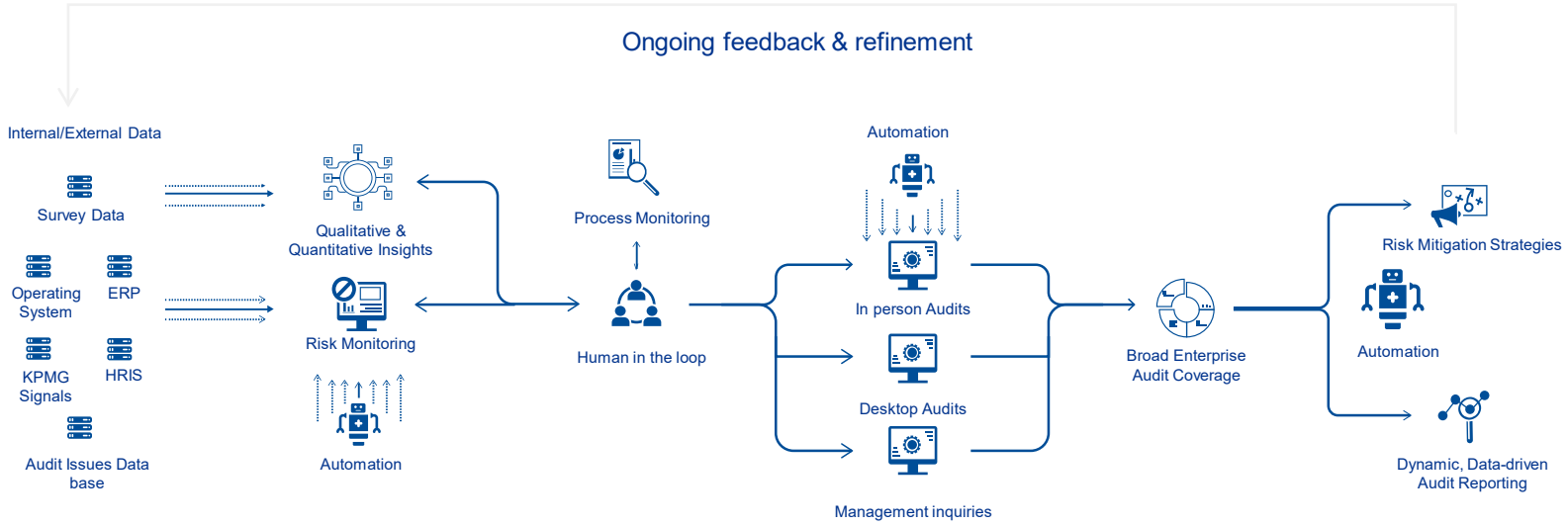
"For a majority of U.S. CEOs, the pandemic has meant an acceleration in digital transformation by months or even years. The move to digitization has accelerated and the potential benefits are expected to be permanent. There is no going back."

— Carl Carande, Vice Chair for Advisory at KPMG in the US.

Strive to thrive amid disruption

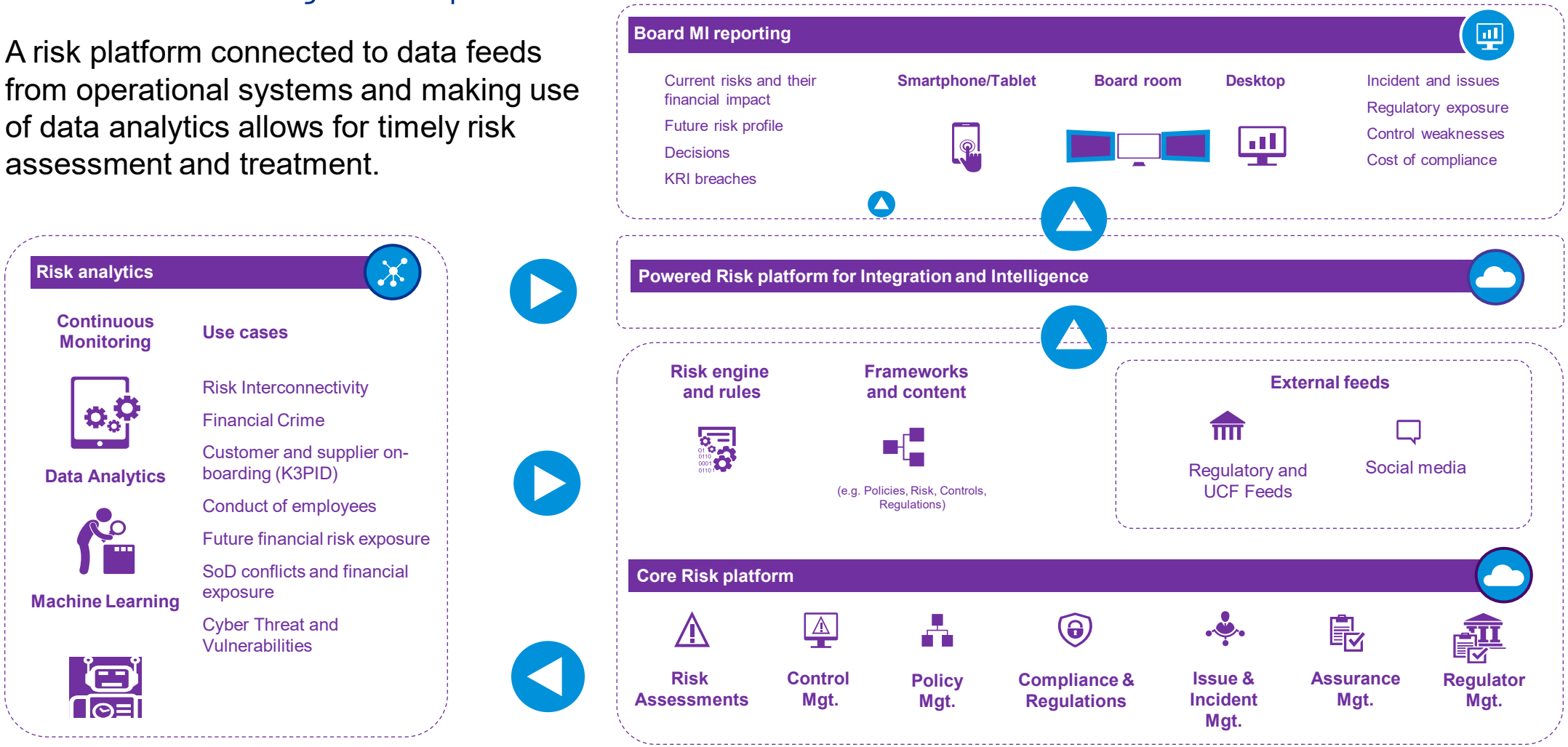
- Internal audit technology is selected with organizational goals in mind to provide as much integration and synergy as possible
- Audit work is enabled via automation and technology at program and project levels
- Internal audit supports business objectives for digital acceleration through AI controls and assurance over digital initiatives and transformation

A glimpse into KPMG firms' digital internal audit story



Future ready risk platform architecture

A risk platform connected to data feeds from operational systems and making use of data analytics allows for timely risk assessment and treatment.



Key Takeaways

1. **Simplifying** the security architecture

2. **Centralised** and **Real-time** policy enforcement and ongoing, **dynamic** and context-based enforcement.

3. **Data availability** for all three lines of defense and reusability of tools.

4. **Automation** of assessments for all three lines of defense (performance, risk, control effectiveness).

5. Timeliness of data and therefore **timely insights and forecasts**, staying relevant.

6. Zero trust is asset and value focused, which makes **risk and control discussions** with the business **easier**.

7. But! Risk and audit need to upskill in **Data Analytics skills** and understanding of new control environments.

8. **Risk and audit** are key stakeholders in a Zero Trust roll-out.

Contact us

Pepijn Kok
Director
Cyber Security
Advisory

Nathamon Wongsala
Associate Director
Technology Risk
Advisory

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia